Certificação Digital através do algoritmo RSA

Samaris Ramiro Pereira[1]

Resumo:

O algoritmo RSA é um padrão mundial tanto para confidencialidade como para certificação digital de usuários e servidores de rede. Ele utiliza conceitos fundamentais da criptografia moderna, sendo alicerce para pesquisas na área. Este artigo orienta a implementação RSA segura em certificações digitais, visto que a maior vulnerabilidade RSA se encontra na inobservância dos cuidados a serem seguidos e estes, se modificam constantemente, acompanhando a evolução das tecnologias da computação.

Palavras-Chave: Assinatura Digital; Certificação Digital; Chave Pública; RSA.

Abstract:

The algorithm RSA is a world pattern for confidentiality and for users' digital certification and net server. It uses fundamental concepts of the modern cryptography, being foundation for researches in the area. This article guides the implementation RSA holds in digital certifications, because the largest vulnerability RSA is in the inobservance of the cares they follow, and these constantly modify, accompanying the evolution of the technologies of the computation.

Keywords: Digital Signature; Digital Certification; Public Key; RSA.

1. Introdução

Cada vez mais a informação passa para o meio eletrônico, facilitando o armazenamento e o compartilhamento, mas também a falsificação. A criptologia é a tecnologia mais adequada para fornecer segurança à informação em aspectos como integridade, confidencialidade e autenticidade de dados e de entidade sendo indispensável em soluções envolvendo Certificação Digital.

---

[1] Mestre em Informática, Bacharel em Matemática com ênfase em Processamento de Dados, Tecnóloga em Técnicas Digitais. Professora da graduação da Fatec-SB, SBC, e da pós-graduação da Faculdade Anchieta, SBC.

Este artigo analisa a segurança da certificação digital implementada através do algoritmo criptográfico RSA, solução utilizada na ICP-Brasil[2], que determina a utilização do RSA na AC-Raiz[3]. A metodologia (Lakatos, 1985) utilizada para a elaboração deste artigo foi a de pesquisas bibliográficas na área, constituída de livros, artigos de periódicos e de materiais disponibilizados na internet, em páginas idôneas. O algoritmo RSA é um padrão mundial em criptografia de chaves públicas, tanto para confidencialidade, como para assinatura digital certificando usuários e servidores de rede.

2. Assinatura e Certificação Digital

A segurança de informação tem por objetivo assegurar uma ou mais das propriedades:

2.1. Confidencialidade – assegura que o acesso a determinada informação seja obtido somente pelo usuário autorizado;

2.2. Integridade – garante que a informação não foi modificada;

2.3. Disponibilidade – garante o acesso a informação quando esta for requerida por um usuário legítimo;

2.4. Autenticação – garante que a identidade é aquela que alega ser;

2.5. Não repúdio – garante que uma terceira parte neutra possa ser convencida de que determinada transação de uma informação ocorreu ou não;

2.6. Legalidade – garante a validade jurídica da informação.

Assinatura manuscrita é um sinal gráfico pessoal emitido de próprio punho para firmar um documento indicando sua aprovação ou autoria. Assinatura eletrônica (ou digitalizada) é apenas a representação eletrônica de uma assinatura manuscrita (Pereira, 2008).

---

[2] Infra-estrutura de Chaves Públicas Brasileira, uma cadeia hierárquica e de confiança governamental, que viabiliza a emissão de certificados digitais para identificação do cidadão quando transacionando no meio virtual, como a Internet (ICP-Brasil, 2009).

[3] Autoridade Certificadora Raiz, centralizadora da certificação digital governamental do Brasil (ICP-Brasil, 2009).

Assinatura Digital é a tecnologia de segurança da informação que garante eletronicamente a integridade (2.2), o não repúdio (2.5) e a autenticação (2.4) dos dados e do signatário em questão. Ela ainda pode opcionalmente garantir confidencialidade (2.1). Legalmente (2.6) a aceitação da assinatura digital não é universal, mas sua aceitação tem evoluído velozmente.

A credibilidade de um documento tradicional (em papel) está ligada à sua originalidade, sendo observadas autoria e integridade do documento. O conceito de assinatura digital abrange estes dois aspectos, garantindo de forma indubitável a autoria do documento (não repúdio) e também que o documento eletrônico não foi alterado (integridade).

Hipoteticamente, uma assinatura manuscrita é única para cada indivíduo, uma assinatura digital não. Além de estar relacionada a uma entidade emissora, uma assinatura digital se relaciona à transação em questão, sendo única para cada transação realizada pelo emissor e tendo sempre um prazo de validade determinado.

Para possibilitar a utilização de assinaturas digitais para transações comerciais e governamentais, foi criada e aperfeiçoada, ao longo do tempo, uma infra-estrutura de chaves públicas (**ICP**), envolvendo padronizações, normas, procedimentos, orientações e leis. Envolvem ainda órgãos como autoridades registradoras (AR), autoridades certificadoras (AC) e outros.

Não há necessidade de se processar a assinatura digital da mensagem completa. Para tornar o custo de tempo de processamento da assinatura digital mais eficiente, a assinatura digital é gerada a partir do valor de *hash*[4] da mensagem.

As assinaturas digitais atuais baseiam-se em criptografia assimétrica (de chaves públicas), conceito essencial para as assinaturas digitais, introduzido por Diffie e Hellman, em 1976 (Diffie e Hellman, 1976). A criptografia assimétrica, ou de chaves públicas, opera com um par de chaves:

[4] Uma função de *hash h* é definida por uma entrada x de tamanho arbitrário finito, considerando $|x|$ o tamanho máximo da entrada, a saída $h(x)$ com tamanho fixo de $|h(x)|$ bits, com $|x| >> |h(x)|$. Nas funções de *hash* criptográficas, dado um valor de *hash*, é intratável encontrar-se outra mensagem que origine o mesmo valor de *hash:* se o tamanho em bits do valor de *hash* for n, a probabilidade de $h(x)$ ser um valor em específico é de 2^{-n} e a probabilidade de colisão é de $2^{-n/2}$ (Pereira, 2008).

Chave Pública - destinada a cifrar a informação, de conhecimento geral;

Chave Privada - de conhecimento apenas do proprietário, destinada a decifrar a informação cifrada pela respectiva chave pública.

O conhecimento da chave pública não deve possibilitar o acesso à chave privada.

A assinatura digital é gerada pela entidade autora, ao assinar o documento eletrônico com a sua chave privada. Deste modo, pode-se verificar a integridade do documento assinado digitalmente, utilizando-se a chave pública da entidade autora e tendo-se a certeza de quem foi que gerou o documento, visto que somente a chave privada deste autor poderia gerar uma assinatura que fosse acessada através de sua respectiva chave pública.

O algoritmo de chaves públicas RSA é o mais amplamente aceito e confiável nas implementações de assinaturas digitais, e pelo grande número de implementações, esta situação tende a durar inclusive porque sua utilização tem crescido ainda mais desde que expirou a validade da sua patente norte-americana, em 2000 (Pereira, 2008).

A certificação digital certifica a autenticidade da assinatura digital combinando aspectos tecnológicos e jurídicos. Ela vem sendo utilizada no Brasil para atribuir valor legal a documentos eletrônicos e para garantir sua eficácia probatória (não repúdio) (ICP-Brasil, 2009).

A vulnerabilidade dos ambientes eletrônicos torna-se evidente à medida que, cada vez mais, importantes operações migram para o mundo digital, meio em que se desenvolvem os mais criativos ataques. A segurança é, portanto, a condição fundamental da eficácia probatória. O desenvolvimento da segurança da informação é sem dúvida, uma necessidade. A cada dia aumentam as organizações no Brasil que utilizam a assinatura e certificação digital, entre elas, bancos para transações on-line, cartórios para autenticações eletrônicas, órgãos judiciários para trâmite de processos, o governo federal para despachos entre a Presidência da República e os ministérios e a Receita Federal para relações com o contribuinte.

3. Infra-estrutura de Chaves Públicas.

Uma infra-estrutura de chaves públicas (ICP) regulamenta a certificação de assinaturas digitais, possibilitando um certificado digital com validade jurídica. Ela combina aspectos tecnológicos e jurídicos, sendo utilizada para atribuir valor legal a documentos eletrônicos garantindo sua eficácia probatória (não repúdio) e se aplicando para documentos eletrônicos de diferentes tipos de informação tais como textos, imagens ou vozes.

No Brasil esta infra-estrutura é definida pela ICP-Brasil (ICP-Brasil, 2009) e controlada pelo ITI (Instituto Nacional de Tecnologia da Informação, 2009), autoridade certificadora raiz (primeira autoridade da cadeia de certificação brasileira – AC Raiz), uma autarquia federal vinculada à casa Civil da Presidência da República que tem como função credenciar as ACs e as ARs através de supervisão e auditorias. A ICP-Brasil é responsável pelo conjunto de técnicas, práticas e procedimentos a serem implementados pelas organizações, com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chaves públicas.

Pelas leis brasileiras em vigor, toda AC deve utilizar-se de chave RSA de comprimento de no mínimo 2048 bits, devendo este valor ser revisto periodicamente, de acordo com as novas definições publicadas pelo CG ICP-Brasil (Comitê Gestor da ICP-Brasil) (ICP-Brasil, 2009). Existem diversos tipos de certificados digitais, sendo classificados quanto à necessidade de segurança da assinatura digital e necessidade de sigilo, mas independente do nível de segurança ou de sigilo, a AC deve assegurar que o tamanho das chaves das entidades a ela ligadas seja de no mínimo 512 bits, sendo recomendável o uso de pelo menos 1024 bits.

Embora as regras de infra-estrutura de chaves públicas não sejam universais, no Brasil, nenhuma AC, nem mesmo a AC-Raiz tem acesso à chave privada da entidade proprietária de um par de chaves públicas. Este par de chaves (pública e privada) deve ser gerado pela entidade usuária, a qual deve zelar por sua chave privada, sendo responsável judicialmente por sua utilização mesmo que por terceiros.

A fim de garantir a segurança da infra-estrutura de chaves públicas, há a necessidade de cuidados na distribuição dos pares de chaves (pública e privada),

evitando assim ataques como o ataque MITM. Neste tipo de ataque, o invasor interage entre duas partes que estejam se comunicando, sem que nenhuma das partes perceba o que está ocorrendo.

Suponha que um adversário obtenha um par de chaves (pública/privada) para utilizar no ataque e que de alguma forma ele consiga trocar a chave pública de *A* pela sua. O adversário passa a monitorar a linha de comunicação. Quando for enviado para *A* um criptograma, o adversário intercepta o canal tendo acesso ao criptograma e não deixa que ele chegue ao destinatário *A*. O adversário decifra o criptograma, altera a mensagem conforme sua conveniência e a envia para *A* com a chave pública correta de *A*, de forma que *A* consiga abrir a mensagem. Da mesma forma, quando *A* enviar uma assinatura digital, o adversário intercepta a mensagem enviada e a substitui por outra que ele cria conforme sua conveniência e divulga como se fosse assinada por *A*.
Para evitar esse tipo de ataque, as AC´s operam como uma terceira parte confiável, certificando a validade do par de chaves no momento da sua criação.

Outra necessidade técnica para a segurança em assinaturas digitais é a utilização de algum esquema de codificação, que processe algum tipo de codificação na mensagem que será assinada, tornando-a pseudo-aleatória e evitando assim, possíveis ataques por mensagem escolhida[5].

4. Algoritmos Criptográficos de Chaves Públicas e o RSA

Desde que foi apresentado o conceito de chaves públicas (Diffie e Hellman, 1976), diversos sistemas de chaves públicas foram criados. Alguns apresentaram quebras na segurança. Outros apresentaram grande dificuldade de implementação. Atualmente, três tipos de sistemas criptográficos de chaves públicas predominam no mercado, os quais se baseiam em problemas envolvidos com funções unidirecionais com segredo: o problema da fatoração de inteiros, o problema do logaritmo discreto sobre corpos finitos e o problema do logaritmo discreto sobre curvas elípticas.

5 O criptoanalista pode escolher determinada(s) mensagen(s) e ter acesso ao(s) par(es) (criptograma; mensagem).

Apesar do RSA estar relacionado com mais de um problema encontrado em funções unidirecionais com segredo, ele é o exemplo mais conhecido de algoritmo de chaves públicas que utiliza o problema da fatoração de inteiros. Ele permite troca de chaves, criptografia e assinatura digital, sendo mais completo do que o algoritmo DSA que permite apenas assinatura digital e o algoritmo Diffie-Hellman permite apenas troca de chaves. Apesar do algoritmo ElGamal permitir troca de chaves, criptografia e assinatura digital, ele é bem menos utilizado do que o algoritmo RSA.

Comparando o RSA com algoritmos de curvas elípticas, observa-se que existem diversas patentes relacionadas a cálculos específicos para algoritmos com curvas elípticas e a patente norte-americana do RSA original está expirada desde 2000. Algoritmos com curvas elípticas podem prover o mesmo nível de segurança que o RSA com chaves menores, sendo mais eficientes do que o RSA na assinatura e deciframento, porém, são mais lentos para cifrar e verificar assinaturas digitais. Outro aspecto a ser comparado é que, devido à data de criação dos algoritmos com curvas elípticas serem recentes em relação ao RSA, a segurança do RSA foi muito mais testada do que a dos algoritmos com curvas elípticas.

O algoritmo RSA é um padrão mundial e suas aplicações são muitas como, por exemplo, no pacote de segurança da Linguagem Java, no Protocolo SSL e no aplicativo OpenSSL. É utilizado também no software de comunicação Skype e no software para criptografia PGP (Pereira, 2008).

O algoritmo RSA é utilizado também na infra-estrutura de chaves públicas brasileira e é o único algoritmo de chaves públicas que pode ser utilizado pela AC-Raiz, a raiz das Autoridades Certificadoras de assinaturas digitais no Brasil (ICP-Brasil, 2009).

5. O algoritmo RSA

O RSA foi desenvolvido em abril de 1977 (Rivest *at al.*, 1978), pelos professores do MIT Ronald **R**ivest e Adi **S**hamir e pelo professor da USC Leonard **A**dleman, batizado com as iniciais de seus nomes.

A patente para o algoritmo RSA (patente 4.405.829 norte-americana) foi emitida em 20 de setembro de 1983, com licença exclusiva para a RSA Security Inc. por meio do Massachusetts Institute of Technology, com data de expiração para 20 de setembro de 2000, incluindo além da confecção de produtos com o algoritmo, sua utilização e sua venda, mas a RSA permitiu durante todo este período, a utilização não comercial gratuita do algoritmo, principalmente para uso acadêmico em docência e pesquisas.

No dia 6 de setembro de 2000, a RSA Security Inc. renunciou a patente e tornou público o algoritmo, porém, existem variações do algoritmo RSA patenteadas por outros proprietários e com licença em vigor. Em hardware, o RSA pode ser encontrado em cartões inteligentes e em linhas telefônicas seguras.

O RSA permite: ciframento e deciframento de mensagem, no conceito de chaves públicas; a geração e a verificação de uma assinatura digital e a combinação dos itens anteriores.

Em 1999, Boneh afirmou que a estrutura do RSA não precisou ser alterada desde a sua criação, pois os ataques encontrados são exemplos de utilizações inadequadas, podendo ser evitados com a escolha dos parâmetros apropriados (Boneh, 1999). Esta afirmação continua válida atualmente.

O algoritmo RSA gera a chave pública e a chave privada a partir de números primos grandes, sendo computacionalmente intratável obter a chave privada a partir da chave pública. O tamanho ideal dos fatores primos do módulo RSA varia conforme a necessidade de cada aplicação. Quanto maior forem os números primos usados para a criação das chaves, maior será a segurança proporcionada por esse algoritmo e menor será o seu desempenho.

O RSA utiliza três funções unidirecionais com segredo:

- Dificuldade da fatoração de número compostos grandes: Função exposta a ataques por fatoração: dado dois números primos grandes, p e q, é tratável se calcular $n=pq$, porém, fatorar n a fim de descobrir p e q é computacionalmente intratável.
- Dificuldade de se encontrar a raiz e-ésima discreta: Função exposta a ataques por criptograma conhecido: calcular uma exponenciação em módulo n é tratável: $c=m^e \bmod n$, mas determinar m sendo a raiz *e-ézima* de $\bmod n$, é

computacionalmente intratável, a menos que se tenha conhecimento do inverso multiplicativo de $e \bmod \varphi(n)$ ou da fatoração de n.

- Dificuldade de se calcular logaritmos discretos módulo n: Função exposta a ataques por mensagem conhecida: dado que $m = c^d \bmod n$, tem-se que $\log_c m = \log_c c^d = d$, então $d = \log_c m$.

Na década de 90, o problema do logaritmo discreto foi muito pesquisado, porém os mais eficientes algoritmos para cálculo de logaritmos discretos possuem complexidade computacional de tempo de processamento semelhante aos algoritmos de fatoração mais eficientes no momento. Geralmente, o logaritmo discreto em um grupo arbitrário de tamanho n possui complexidade $O(\sqrt{n})$ (Pereira, 2008). Geralmente, as implementações RSA seguem as especificações do PKCS #1 ver. 2.1. O PKCS é um conjunto de documentos com especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas de segurança de várias partes do mundo, que visa acelerar por meio de padronização a utilização e desenvolvimento de algoritmos de chaves públicas. O PKCS surgiu em 1991 como um resultado de encontros com um pequeno grupo de pessoas precursoras no uso da tecnologia de chaves públicas e desde então tem se tornado referência até mesmo para padrões estabelecidos como ANSI X9, PKIX, SET, S/MIME e SSL. Atualmente seu desenvolvimento ocorre basicamente via lista de discussões e *workshops* ocasionais (RSA Security Inc., 2009).

A última versão do PKCS #1 é a versão 2.1, de 14 de junho de 2002. A versão mais antiga do PKCS #1, entre as disponíveis pelas publicações dos Laboratórios RSA, é a versão 1.5, de 1 de novembro de 1993. O padrão para assinatura digital especificada no PKCS #1 ver. 1.5 é vulnerável a um ataque descrito por Bleichenbacher e aplicado contra o protocolo SSL ver. 3.0 e, portanto, não deve ser utilizado (RSA Security Inc., 2009).

6. Criação do par de chaves públicas no algoritmo RSA

Para a criação das chaves RSA (Menezes *at al.*, 2001) são escolhidos dois

números primos grandes distintos: p e q. Computa-se o módulo RSA, também chamado módulo n ou simplesmente módulo: $n=pq$. Calcula-se $\varphi(n)=(p-1)(q-1)$.

Escolhe-se um número inteiro positivo e, chamado de expoente público, tal que $1< e< \varphi(n)$, de forma que $\text{mdc}(e, \varphi(n)) = 1$. Determina-se o número d, chamado de expoente privado, tal que $ed-1$ seja divisível por $\varphi(n)$.

O par (e, n) é a chave pública e o par (d, n) é a chave privada. Os valores p e q devem ser mantidos em segredo. O ciframento é dado por $c = m^e \bmod n$, sendo m representação numérica (em números inteiros positivos) do texto legível, dividido em blocos menores que n. O deciframento é dado por $m = c^d \bmod n$.

A escolha dos primos p e q e do expoente público e, deve ser cuidadosa.

Existem variações RSA do algoritmo RSA. Uma variação de um algoritmo criptográfico consiste em uma modificação realizada na definição original deste, a fim de trazer algum benefício ao processo, seja este de segurança, de tempo de processamento, de espaço de armazenamento em memória ou outras vantagens. Pode ocorrer em diferentes partes do algoritmo e atingir objetivos distintos. Devido ao tempo de existência do RSA, surgiram variações da definição inicial e algumas foram adotadas como padrão em normas técnicas. Não há análise para se determinar qual a melhor variação RSA. Cada variação visa um determinado objetivo. Deve-se analisar a melhor opção de variação para a implementação a ser realizada, levando-se em consideração fatores tais como necessidade de segurança, tempo de processamento, capacidade computacional, possibilidade de investimento e necessidades de pagamento de taxas relativas a patentes.

A escolha inadequada de parâmetros RSA, a divulgação dos mesmos e outros erros de implementação possibilitam ataques ao RSA, assim como o ataque MITM, que pode ocorrer na distribuição de chaves de qualquer algoritmo de chaves públicas. Cada ataque exige uma detalhada análise dos cuidados necessários para que este não obtenha sucesso. Um único cuidado que seja esquecido torna a implementação RSA vulnerável. Em caso de utilização de variações do RSA, devem-se observar os cuidados específicos

para esta variação. É importante também, estar atento a novas publicações sobre o tema, visto que podem surgir novos ataques ao algoritmo.

A segurança do RSA depende ainda, da intratabilidade da fatoração de números inteiros. Existem dois tipos de algoritmos de fatoração: os de propósito especial e os de propósito geral. Os algoritmos de fatoração de propósito especial dependem do tamanho dos fatores desconhecidos do número inteiro n que se deseja fatorar, de forma que, sua eficiência, depende do tamanho do menor fator primo de n. Este tipo de algoritmo é mais eficiente para fatorar números que possuem fatores primos pequenos (com até 256 bits) do que para fatorar números que possuem fatores primos balanceados. Os algoritmos de fatoração de propósito geral dependem do tamanho do número n que se deseja fatorar.

O RSA utiliza uma teoria matemática elegante, sendo que a análise dos fundamentos matemáticos possibilita a sua correta implementação, confiança na sua segurança, é embasamento para a criação de variações e alicerce para estudos mais sofisticados. A maior vulnerabilidade do RSA se encontra na falta de atenção quanto aos cuidados a serem observados ao se desenvolver uma aplicação que utilize o algoritmo RSA, envolvendo implementação, escolha das chaves e utilização do algoritmo. A análise detalhada desses cuidados pode ser encontrada em Pereira, 2008.

7. Conclusão e Problemas de Pesquisa em Aberto

Devido à longa existência e ao volume de pesquisas realizadas no algoritmo RSA, novas pesquisas exigem um elevado conhecimento matemático e computacional. Existem problemas em abertos tais como (Pereira, 2008):

- Proposta de teste de primalidade determinístico com tempo computacional menor do que o algoritmo AKS, o mais eficiente no momento, apresentando custo computacional de tempo de processamento $O(lg^{19}\, n)$ operações binárias;
- Proposta de algoritmo para fatoração de propósito geral mais eficiente que o NFS, o mais eficiente no momento;
- Proposta de algoritmo para fatoração de propósito especial mais eficiente que o ECM, o mais eficiente no momento;

- Proposta de algoritmo eficiente para cálculo da raiz e-ésima módulo *n*;
- Proposta de algoritmo para cálculo de logaritmo discreto módulo *n* mais eficiente do que os existentes atualmente;
- Proposta de variações do algoritmo RSA que apresente algum benefício em relação às variações atuais como, por exemplo, maior eficiência no deciframento e ciframento ou utilização de chaves menores;
- Proposta de novo ataque ao algoritmo RSA que explore fraquezas diferentes das três funções unidirecionais com segredo com compõem o estado da arte RSA;
- Análise da repercussão de novas tecnologias sobre o algoritmo RSA como, por exemplo, o aumento da capacidade computacional ou a proposta de um novo algoritmo de fatoração.

O algoritmo criptográfico RSA é um padrão mundial entre os algoritmos criptográficos de chaves públicas, tanto para confidencialidade, como para assinatura digital. Suas aplicações são atuais e muitas, e estão aumentando ainda mais, após ter expirado a patente americana do algoritmo.

O conteúdo das pesquisas desenvolvidas desde o anúncio do RSA se encontra dispersa devido ao volume e ao tempo, incluindo uma época na qual estas pesquisas não contavam com o recurso da divulgação eletrônica via Internet, o que gerou algumas pesquisas redundantes. Este fato contribui com a maior vulnerabilidade do RSA, a falta de conhecimento e atenção quanto aos cuidados a serem observados ao se desenvolver uma aplicação que o utilize. E estes cuidados crescem gradativamente com o anúncio de novos ataques, com o crescimento da capacidade de processamento computacional e outros. Neste contexto, é necessária uma atualização quanto aos cuidados necessários para implementação RSA cada vez que esta for utilizada, independente do período em que houve a última atualização.

8. Referências.

Boneh, D. *Twenty years of attacks on the RSA cryptosystem*: *journal Notices of the American Mathematical Society*, v. 46, n. 2. 1999.

Diffie, W.; Hellman, M. E. *New Directions in Cryptography* (1976): Cambridge University Press, IEEE International Symposium on Information Theory in Ronneby, Sweden. 2005.

ICP-Brasil. Infra-estrutura de Chaves Públicas Brasileira. Disponível em: http://www.icpbrasil.gov.br/. Acesso em 10/05/2009.

Instituto Nacional de Tecnologia da Informação. Autoridade Certificadora Brasileira Raiz – ITI. Disponível em: http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao, Acesso em 10/05/2009.

Lakatos, E. M.; Marconi, M. A. Fundamentos de Metodologia Científica. 4 ed. São Paulo, Ed. Atlas. 1985.

Menezes, A. J.; Oorschot, P. C.; Vanstone S. A. *Handbook of Applied Cryptography*, 1ª ed. CRC Press. 2001.

Rivest, R. L.; Shamir, A.; Adelman, L. M. *A method for obtaining digital signatures and public-key Cryptosystems*: *Communications of the* ACM, 21, 120-126. 1978.

Pereira, S. R. O Sistema Criptográfico de Chaves Públicas RSA: Dissertação apresentada à Universidade Católica de Santos, UNISANTOS. 2008.

RSA Security Inc. Laboratórios RSA. Disponível em: http://www.rsasecurity.com/rsalabs/. Acesso em 10/05/2009.